POLICY 2.501

4-E I recommend that the Board adopt the proposed new Policy 2.501, entitled "Information Security – Access Control Policy."

[Contact: Deepak Agarwal, PX 48773 and Larry Padgett, PX 48830.]

Adoption **CONSENT ITEM**

- The Board approved development of this revised Policy at the development reading on May 26, 2010.
- This policy sets forth access to information systems and services on the basis of business and information security requirements, as well as to meet any requirements of state or federal law. Additionally, it sets forth:
    - o User IDs creations
    - o Access controls for Network and servers
    - o Password standards
    - o Minimum access rights
    - o Separation of duties
    - o Periodic review of User access
    - o Regulations on unattended computers
    - o Controls for physical access

See Item 4D/Policy 8.123 for the referenced IT User Standards and Guidelines Manual.

POLICY 2.501

INFORMATION SECURITY - ACCESS CONTROL POLICY

1. **Purpose:** To control access to information. Access to information systems and services should be controlled on the basis of business and information security requirements as well as to meet any requirements of state or federal law. This Policy does not prohibit or restrict public access to inspect data and information on publicly available District technology resources.

2. **Definitions:** The IT User Standards and Guidelines Manual provides definitions of terms used within this Policy. This Manual is incorporated herein by reference as part of this Policy and can be located on the District's IT Security web site at: http://www.palmbeachschools.org/it/security.asp.

3. **Policy:**

   a. User Access Management.

      i. All users, except third party users and as stated below, will be automatically assigned a unique User ID for their use only. As to third party users, they will be assigned a User ID, on request by their District contact/coordinator, when in the best interest of the District. Further, all users will have a password. Yet, as to students, see School Board Policy 8.123, sub-paragraphs (2) (d) & (e), relating to passwords and User ID's.

      ii. Access to the network/servers and information systems will be by User ID and password and, in appropriate cases, a secondary authentication method may be necessary, such as a smartcard, PIN number or biometric data.

      iii. IT shall utilize appropriate information system controls to enforce the password standards defined in the IT User Standards and Guidelines Manual.

      iv. Users will only be given sufficient rights to all systems they have been specifically approved and authorized to use based on the District's business and information security requirements, as well as to meet any requirements of state or federal law. Access is also controlled by the District's web site filtering policy—School Board Policy 8.125.

      v. User rights will be kept to a minimum at all times. Employees shall be given, by default, basic access to e-mail and calendaring services and appropriate self-service HR services, such as eBenefits and ePay.

vi. Users requiring access, other than basic, to information systems must make the requests for access according to processes defined by each information system owner.

vii. The information system owner shall be identified and will determine user access rights for their systems. Information system owners shall consider separation of duties when determining user access rights.

viii. System administration rights to information systems, including network devices, shall be restricted to the appropriate users based on the District's business and information security requirements.

ix. The user's User ID shall be immediately disabled when a resignation or termination change in his/her status occurs in PeopleSoft the District's Human Resource system. ~~, such as resignation or termination, has occurred.~~

x. User's access rights shall be periodically reviewed to make sure the access is approved and authorized based on the District's business and information security requirements.

b. Physical Access Management.

i. Users must not leave their computer or other access unit unattended during normal work hours without first logging off or invoking a password protected screen saver.

ii. Users must turn off their computers or other access units at the end of normal work hours. If a computer or other access unit must stay on after normal work hours, precautions shall be taken to prevent unauthorized use.

iii. Physical access into facilities that contain information systems, such as computer rooms and data storage areas, shall be restricted to those people that are approved and authorized based on the District's business and information security requirements. Physical access shall be controlled using methods such as walls, locks, key card systems, and biometric readers.

iv. Physical access into controlled facilities shall be logged and monitored.

STATUTORY AUTHORITY: Fla. Stat. §§ 1001.32(2); 1001.41(2); 1001.42(26); 1001.43(1)
LAWS IMPLEMENTED: Fla. Stat. §§ 1001.32(2); 1001.43(3); 1001.42(8) & (9); 1003.31; 1006.28(1)
HISTORY: __/___2010

Legal Signoff:

The Legal Department has reviewed proposed Policy 2.501 and finds it legally sufficient for adoption by the Board.

_____ _____

Attorney Date